International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Cloud-Integrated Locally Deep Ensemble Intrusion Detection for Intelligent and Secure Smart Healthcare Systems

P. Hussain[1*], K. Venkata Ramana[1], K. Rahul[1], T. Deepak[1], Chegonda Krishna Vamshi[1], Dommata Karthik Reddy[1]

[1]Department of Electronics and Communication Engineering, Kommuri Pratap Reddy Institute of Technology, Ghanpur, Ghatkesar, 501301, Telangana, India.

*Correspondence: P. Hussain

ABSTRACT

The expansion of smart healthcare technologies and interconnected IoMT infrastructures has intensified the need for advanced, secure, and scalable analytical solutions. As modern systems increasingly rely on cloud-based and distributed environments, maintaining high prediction performance and effective anomaly detection has become more complex, particularly when handling large-scale and imbalanced datasets. Conventional methods typically depend on isolated models and manual processing, which often leads to suboptimal accuracy, limited adaptability, and poor handling of data imbalance, thereby restricting their applicability in real-time scenarios. To address these challenges, this work introduces a cloud-oriented intelligent framework that integrates machine learning within a distributed client–server setup to enable secure and efficient predictive analysis. In this architecture, LP1 functions as the server hosting the prediction engine, while LP2 operates as the client for remote interaction. The system incorporates data preprocessing through label encoding (LE) and addresses class imbalance using the Synthetic Minority Oversampling Technique (SMOTE). It employs multiple baseline models, including Ridge Classifier (RC), Quadratic Discriminant Analysis (QDA), and Perceptron, alongside a proposed Locally Deep Ensemble Classifier (LDEC), which combines Histogram Gradient Boosting Classifier (HGB) and Light Gradient Boosting Machine Classifier (LGBM) using soft voting (SV). Furthermore, Redis-based authentication ensures secure access control. The overall framework significantly improves predictive performance, robustness, scalability, and system security for next-generation healthcare applications.

Key words: Intrusion Detection System, Cloud-Based Security, Cybersecurity in Healthcare, Secure Authentication, Internet of Medical Things.

1. INTRODUCTION

The widespread growth of the Internet has given rise to the Internet of Things (IoT), a transformative concept that supports the creation of intelligent and connected environments in diverse areas such as smart homes and urban infrastructures [1]. Building upon this advancement, the incorporation of medical sensors and healthcare devices has driven the development of the Internet of Medical Things (IoMT), aimed at improving patient care, remote monitoring, and overall healthcare efficiency [2]. However, as these systems become increasingly interconnected, they also generate and exchange vast amounts of sensitive medical data, making security a major challenge [3]. To safeguard such environments, Intrusion Detection Systems (IDSs) have become essential, offering both software- and hardware-based mechanisms to detect, analyze, and respond to potential cyber threats that traditional security approaches may fail to identify [4].

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

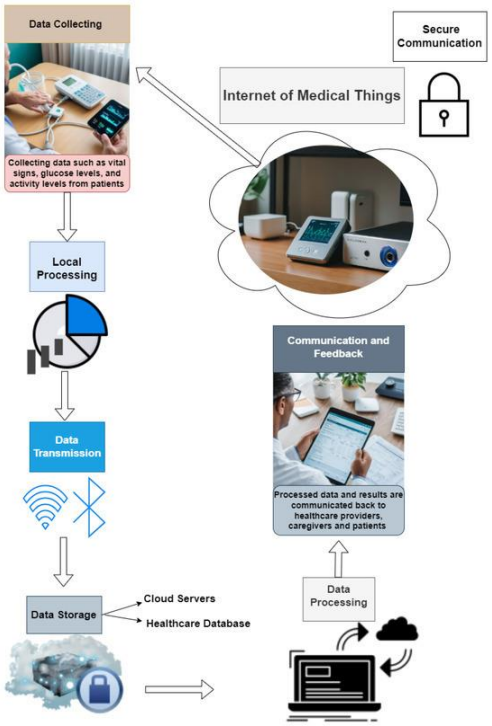

Fig. 1. Intrusion Detection System for Securing Internet of Medical Things

The healthcare sector has experienced significant transformation due to the adoption of IoT and the advancement of IoMT technologies, primarily aimed at improving the quality of patient care and operational efficiency [5]. However, the growing number of connected devices also introduces vulnerabilities, making healthcare systems more susceptible to cyber-attacks. To address these challenges, the application of ensemble learning techniques in intrusion detection systems has gained considerable attention [6]. Ensemble approaches, including bagging, boosting, and stacking, combine multiple base models to improve prediction accuracy and robustness in detecting anomalies within IoT and IoMT networks [7]. The integration of ensemble learning into IDS frameworks provides an effective solution to enhance cybersecurity in healthcare environments [8]. As shown as fig 1. It ensures better protection of sensitive medical data and maintains system integrity despite the increasing complexity of network infrastructures [9]. Furthermore, ensemble-based IDS can adapt to evolving attack patterns by utilizing meta-learning and dynamic decision fusion strategies, thereby improving detection performance under varying network conditions [10].

Smart healthcare systems rely heavily on IoMT devices that continuously collect, transmit, and analyze sensitive physiological data. However, these IoMT environments are highly vulnerable to intrusions such as spoofing, unauthorized access, and malicious data manipulation. Traditional IDS solutions face limitations due to poor handling of data imbalance, low adaptability to dynamic traffic patterns, insufficient computational capacity on IoMT nodes, and a lack of remote predictive capability. Therefore, there is a need to design and develop a cloud-assisted, machine-learning-driven intrusion detection system capable of performing robust preprocessing, balanced training, ensemble prediction, secure authentication, and remote real-time intrusion detection through a distributed architecture involving Admin and User systems.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

2. LITERATURE SURVEY

Mousa Alalhareth et, al. [11] proposed a fuzzy-based self-tuning Long Short-Term Memory (LSTM) intrusion detection system (IDS) for the IoMT. Their approach dynamically adjusts the number of epochs and utilizes early stopping to prevent overfitting and underfitting. They conducted extensive experiments to evaluate the performance of their proposed model, comparing it with existing IDS models for the IoMT.

Arash Salehpour et, al. [12] Proposed the system that decreases the dimensionality by operating the MI filtering on the dataset and keeps only the most informative features. It further refines this using ensemble-based ranking methods, such as Random Forest, AdaBoost, XGBoost, and LightGBM, to ensure the optimum feature selection for the task. Random Forest was adopted for the final classification because it is generally robust, efficient at handling high-dimensional data, and usually performs well. The proposed system has been tested with intensive usage using three well-acknowledged benchmark datasets, namely WUSTL-EHMS-2020, NSL-KDD, and CIC-IoMT2024. It showed considerable accuracy, precision, recall, and F1-score gains, particularly for DDoS and DoS attack types.

Nikhil Sharma et, al. [13] The proposed DA-DRL-AES-SHA-512 methodology significantly outperformed conventional encryption techniques, achieving an encryption time of 0.0975 s, decryption time of 0.0846 s, and a throughput of 75.63 transactions per second (Tx/s) with a network overhead of just 0.1289%. The Energy consumption and computational overhead are reduced to 0.3664 J and 0.48%, respectively. The Secure and Dependable Bi-LSTM GRU Intrusion Detection Framework (S-BiLSTMGRU-IDF) achieved 99.94% accuracy in binary classification and 99.89% in multiclass classification, improving detection efficiency by 0.6–3.5% over state-of-the-art models.

Georgios Zachos et, al. [14] Introduced an AIDS specifically designed for resource-constrained devices within IoMT networks. The proposed lightweight AIDS leverages novelty detection and outlier detection algorithms instead of conventional classification algorithms to achieve (a) enhanced detection performance against both known and unknown attack patterns and (b) minimal computational costs.

Abdelatif Hafid et, al [15] proposed a high-performance cybersecurity framework leveraging a carefully fine-tuned XGBoost classifier to detect malicious attacks with superior predictive accuracy while maintaining interpretability. Their comprehensive evaluation compared the proposed model with a well-regularized Logistic Regression baseline using key performance metrics. Additionally, they analyze the security-cost trade-off in designing ML systems for threat detection and employ SHAP (SHapley Additive exPlanations) to identify key features driving predictions. They further introduced a late fusion approach based on max voting that effectively combines the strengths of both models.

Faeiz Alserhani et, al [16] The system is constructed on a feedback-looped architecture integrating hybrid feature modeling, physical behavioral analysis, and Extreme Learning Machine (ELM)-based classification to provide adaptive access control, continuous monitoring, and reliable intrusion detection. ML-CCPS is capable of outperforming benchmark classifiers with an acceptable computational cost, as evidenced by its macro F1-score of 97.8% and an AUC of 99.1% when evaluated with the ToN-IoT dataset.

Mohammad Zubair Khan et, al. [17] introduced a novel hybrid anomaly detection model combining a Graph Convolutional Network (GCN) with a transformer architecture. The GCN captures the structural relationships within the IoMT data, while the transformer models the sequential dependencies in the anomalies

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Arezou Naghib et, al [18] paper identified 28 critical studies published between 2018 and April 2024. The intrusion detection mechanisms in the IoMT are divided into five categories: IDS based on artificial intelligence models, datasets used in IoMT for IDS, fundamental security requirements, intrusion detection processes, and evaluation metrics. This paper dissects the various mechanisms within each category in a meticulous and comprehensive analysis.

Yahya Rbah et, al. [19] presented a low-cost, high-accuracy ML-based attack detection framework for securing IoMT devices. Eight ML models, including Decision Tree, Support Vector Machine, Naive Bayes, Gradient Boosting, K-Nearest Neighbor, Random Forest, and XGBoost, were evaluated on the IoT-Healthcare security dataset. XGBoost emerged as the top performer, achieving 99.98% accuracy in just 233 ms.

Jordi Doménech et, al. [20] addressed these limitations by comparing the performance of ML models trained on a general IoT dataset (CICIoT2023) and an IoMT-specific dataset (CICIoMT2024) to demonstrate the importance of domain-specific data. Their findings reveal substantial drops of up to 66.87% in the F1-score when models trained on one dataset are tested on the other.

3. PROPOSED SYSTEM

The proposed User Cloud-Driven Intrusion Detection System (IDS) is designed to enhance the security of Internet of Medical Things (IoMT) environments by integrating advanced machine learning techniques with a cloud-based architecture. The system follows a dual-module design consisting of Laptop 1 (LP1) as the server and Laptop 2 (LP2) as the client. On the server side (LP1), the system performs dataset preprocessing, model training, performance evaluation, and deployment of the prediction model. As shown as fig 2. On the client side (LP2), users interact through a graphical interface to securely upload test data and obtain real-time predictions. The integration of a Flask ensures smooth communication between client and server, while Redis-based authentication provides secure login and role-based access control. This architecture enables scalable, automated, and real-time intrusion detection, making it suitable for protecting sensitive IoMT infrastructures against evolving cyber threats.

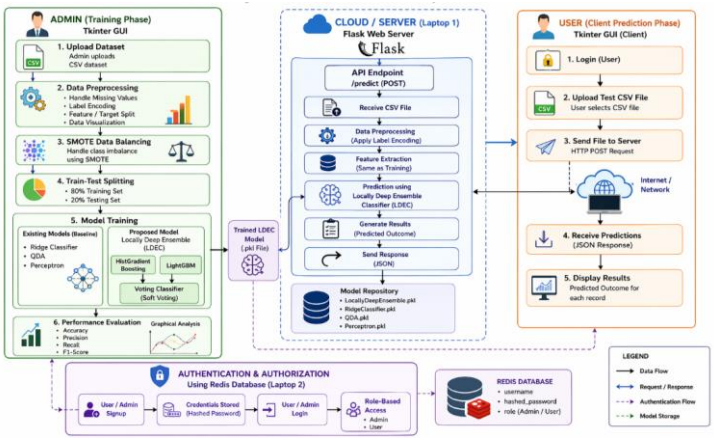

Fig. 2. Proposed System Architecture of anomaly detection in healthcare systems

1. Setup and Library Initialization

- Essential libraries for data processing (pandas, numpy), visualization (matplotlib, seaborn), and machine learning are imported.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- Joblib is used for model persistence, and threading enables parallel execution of GUI and server.
- Redis and hashlib are used for secure authentication and password hashing.
- Custom modules such as MetricsCalculator and GraphPlotter are integrated for evaluation and visualization.

2. Dataset Loading

- The admin uploads the dataset via a Tkinter GUI.
- The dataset is read from a CSV file and displayed for verification.
- This step ensures correctness before further processing.

3. Data Preprocessing

- Missing values are handled and categorical features are encoded using LabelEncoder.
- The dataset is split into features (X) and target (Y).
- A count plot is generated to visualize class distribution.

4. Data Balancing (SMOTE)

- SMOTE is applied to handle class imbalance.
- Synthetic samples are generated for minority classes.
- Graphs compare distributions before and after balancing.

5. Train-Test Splitting

- The dataset is divided into 80% training and 20% testing data.
- This ensures proper evaluation on unseen data.

6. Model Training and Evaluation

- Baseline models: Ridge Classifier, QDA, and Perceptron are trained.
- Proposed model: LDEC combines HistGradientBoosting and LightGBM using soft voting.
- Models are evaluated and stored using joblib.

7. Performance Analysis

- Metrics such as Accuracy, Precision, Recall, and F1-score are calculated.
- Graphs and summaries are generated for comparison.
- The best-performing model (LDEC) is selected.

8. Flask Server Deployment

- The trained LDEC model is deployed using a Flask server.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

- A REST API endpoint (/predict) is created.
- The server processes uploaded data and returns predictions in JSON format.

9. Authentication Using Redis

- Redis stores user credentials securely.
- Passwords are hashed using SHA-256.
- Role-based access (Admin/User) is implemented.

10. Client-Side Prediction (LP2)

- Users log in via GUI and upload test CSV files.
- The file is sent to the server via HTTP POST request.
- The server processes and predicts outcomes.

11. Result Display

- Predictions are displayed in the user interface.
- Server logs track incoming data and outputs.
- Suspicious activities can be identified and monitored.

12. System Summary

- **LP1 (Server):** Handles preprocessing, training, evaluation, and deployment.
- **LP2 (Client):** Provides user interface for prediction.
- **Flask API:** Enables communication between client and server.
- **Redis:** Ensures secure authentication and access control.

LDEC model

The LDEC is the proposed advanced model in this intrusion detection system, designed to combine the strengths of multiple gradient-boosting algorithms into a single, high-performance predictive engine. Unlike individual classifiers that rely on a single decision structure, LDEC integrates multiple learners to capture both deep local interactions and broad global patterns within IoMT network traffic. It achieves this by merging the predictive capabilities of two non-linear, tree-based models HGB and LGBM using a soft-voting strategy that averages their probability estimates. As shown as fig 4.8 This ensemble approach significantly enhances robustness, reduces overfitting, and improves sensitivity to rare intrusion behaviors that may be overlooked by traditional machine learning methods. LDEC is particularly effective for IoMT environments because it adapts well to heterogeneous attributes, imbalanced datasets, and subtle deviations in device behavior, ultimately delivering higher accuracy, stronger generalization, and more stable intrusion detection performance.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

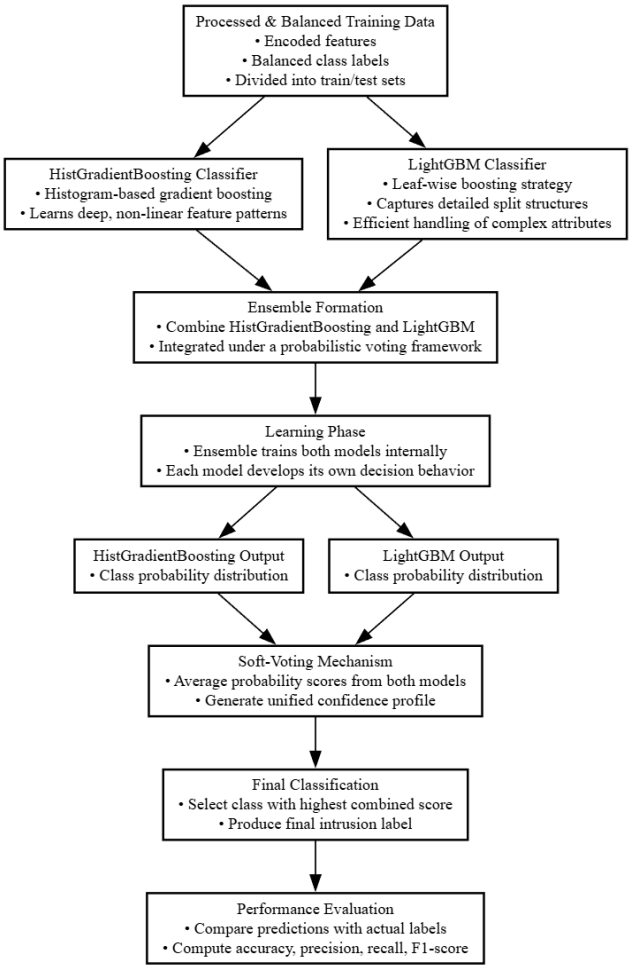

Fig. 3. Internal workflow of LDEC model

The processed and balanced dataset is first prepared by cleaning missing values, encoding categorical features, and splitting it into training and testing sets to ensure reliable learning. Next, two powerful ensemble components—Histogram Gradient Boosting (HGB) and Light Gradient Boosting Machine (LGBM)—are initialized to capture complex and non-linear intrusion patterns present in IoMT traffic data. These classifiers are then integrated into a unified ensemble framework using a probabilistic soft-voting mechanism, allowing them to operate collaboratively. During training, both models independently learn from the same dataset, each constructing its own decision structure. For prediction, each model generates class-wise probability scores representing its confidence for every test instance. Finally, these probability outputs are aggregated through soft voting by averaging the scores from both classifiers, resulting in a robust and consolidated prediction that enhances overall intrusion detection accuracy.

4. RESULT DESCRIPTION

Fig. 4. shows the comparison between class distributions before and after applying the SMOTE algorithm. The left graph indicates the original imbalance where some classes have fewer samples, while the right graph displays equalized class counts post-balancing. SMOTE helps the model learn better by generating synthetic samples for minority classes. This process ensures fairness in model

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

training and reduces bias toward majority classes. It enhances the robustness and overall predictive performance of the IDS model.

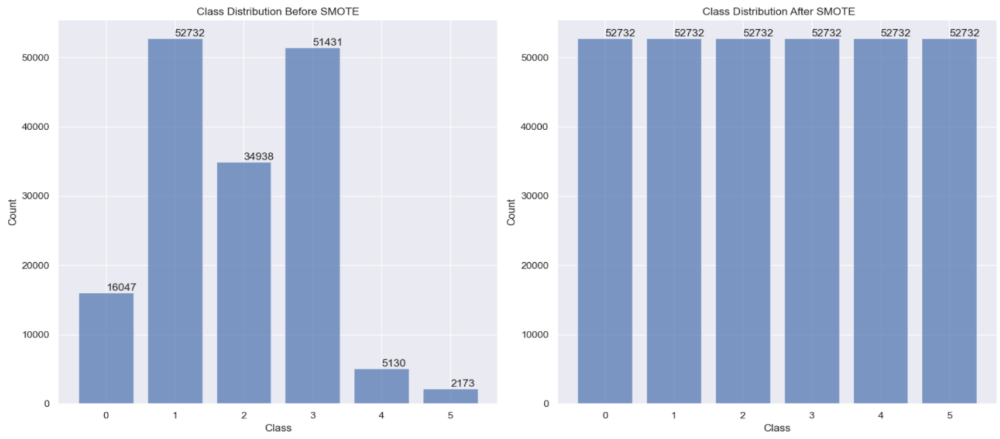

Fig. 4. Class Distribution of Dataset Before and After Applying SMOTE

Fig. 5. illustrates the confusion matrix and ROC curve for the proposed LDEC model, clearly showing dominant diagonal elements representing correctly classified samples. The minimal off-diagonal values indicate very few misclassifications across classes like ARP Spoofing, Benign, and DDoS. This signifies strong feature extraction and decision fusion achieved through local deep ensemble learning and also presents the ROC curves for all classes, each achieving an AUC of 1.00, reflecting perfect class separability and predictive reliability. The model demonstrates consistent performance across every intrusion category, outperforming all traditional classifiers and proving its effectiveness for real-time IoMT intrusion detection.

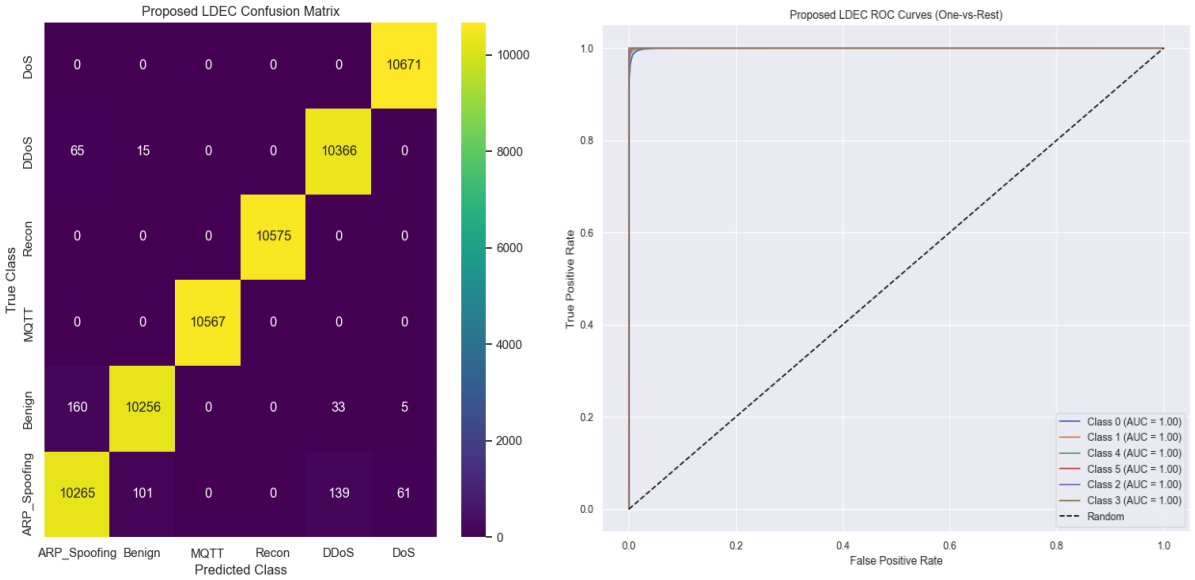

Fig. 5. Illustration of confusion matrix and ROC curve using proposed LDEC model

Fig. 6. shows the admin-side interface that receives the dataset transmitted by the client system. The server decodes the incoming data, processes it through the trained model, and determines the corresponding intrusion category. This setup demonstrates effective cross-device communication in a

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

distributed IoMT environment. It validates the integration of client data with server-side computation. The screen confirms successful data reception and real-time processing.

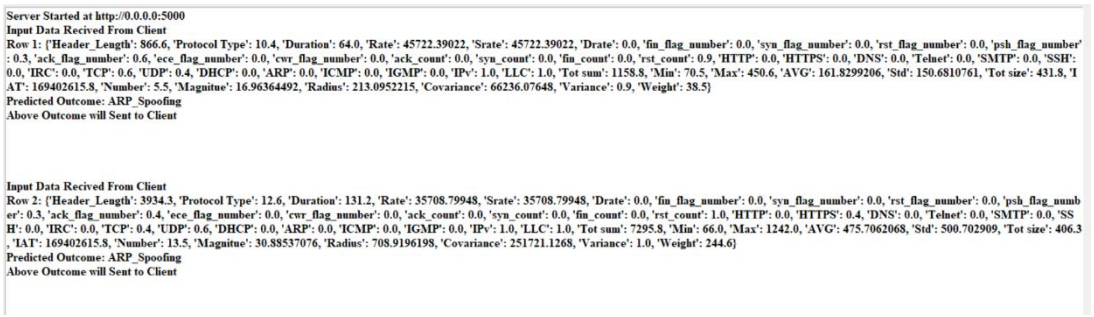

Fig. 6. Cloud Predicting the Test Data of the Client & Transmitting Screen

Fig. 7. represents the user-side interface that receives the prediction results from the admin server. Once the data is processed and classified, the predicted outcomes are transmitted back to the client device. The results indicate detected intrusion types such as DoS, DDoS, or ARP Spoofing. This communication ensures timely alerts and intelligent decision support for users. The setup demonstrates a complete client-server interaction flow, ensuring real-time detection and secure feedback within the IoMT ecosystem.

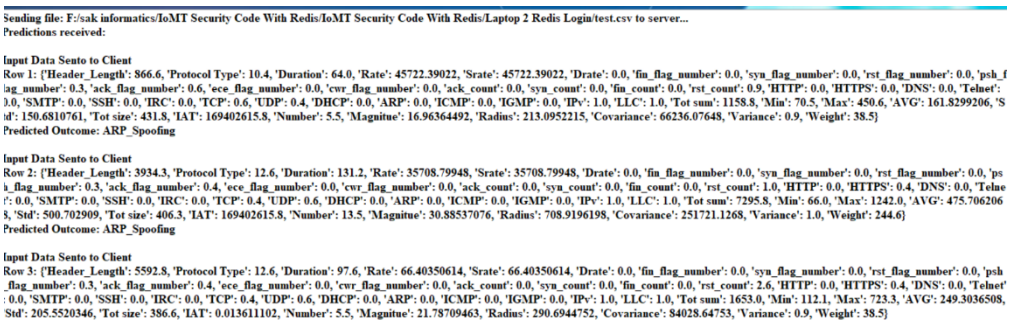

Fig. 7. User Receiving the Prediction output

5. CONCLUSION

The research provides an intelligent, scalable, and efficient solution for enhancing the cybersecurity of connected healthcare infrastructures. By integrating cloud-based analytics with machine learning algorithms such as HGB and LGBM within a Voting Ensemble, the system achieves superior accuracy and robustness compared to traditional models like RC, QDA, and Perceptron. Through effective preprocessing, normalization, and SMOTE-based data balancing, it successfully mitigates data imbalance issues and enhances model generalization across diverse IoMT traffic patterns. The hybrid deployment using Tkinter GUI, Redis-based authentication, and a Flask server ensures real-time user interaction and secure remote predictions. Experimental results demonstrate significant improvements in detection accuracy, recall, and precision, confirming the reliability of the LDEC model. The system contributes a powerful and adaptive intrusion detection framework capable of protecting IoMT environments against evolving cyber threats while maintaining high performance and scalability.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

REFERENCES

[1] Halder, S.; Ghosal, A.; Conti, M. Efficient physical intrusion detection in Internet of Things: A Node deployment approach. Comput. Netw. 2019, 154, 28–46.

[2] Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput. Commun. 2021, 166, 110–124.

[3] Balandina, E.; Balandin, S.; Koucheryavy, Y.; Mouromtsev, D. IoT use cases in healthcare and tourism. In Proceedings of the 2015 IEEE 17th Conference on Business Informatics, Lisbon, Portugal, 13-16 July 2015; IEEE: Piscataway, NJ, USA, 2015; Volume 2, pp. 37–44.

[4] A. Heidari, M.A.J. Jamali Internet of Things intrusion detection systems: a comprehensive review and future directions.Clust. Comput., 26 (2023), pp. 3753-3780, 10.1007/s10586-022-03776-z

[5] Alalhareth, M.; Hong, S.-C. An Improved Mutual Information Feature Selection Technique for Intrusion Detection Systems in the Internet of Medical Things. Sensors 2023, 23, 4971.

[6] Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.C.; Rodriguez, J. An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks. Electronics 2021, 10, 2562.

[7] Ren, J.; Wan, H.; Zhu, C.; Qin, T. Stacking ensemble learning with heterogeneous models and selected feature subset for prediction of service trust in internet of medical things. IET Inf. Secur. 2022, 17, 269–288.

[8] Rahmani, A.M.; Naqvi, R.A.; Ali, S.; Mirmahaleh, S.Y.H.; Alswaitti, M.; Hosseinzadeh, M.; Siddique, K. An Astrocyte-Flow Mapping on a Mesh-Based Communication Infrastructure to Defective Neurons Phagocytosis. Mathematics 2021, 9, 3012.

[9] Khan, S.; Akhunzada, A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). Comput. Commun. 2021, 170, 209–216.

[10] Tauqeer, H.; Iqbal, M.M.; Ali, A.; Zaman, S.; Chaudhry, M.U. Cyberattacks Detection in IoMT using Machine Learning Techniques. J. Comput. Biomed. Inform. 2022, 4, 13–20.

[11] Alalhareth, M.; Hong, S.-C. An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning. Sensors 2023, 23, 9247. https://doi.org/10.3390/s23229247

[12] Salehpour, A., Balafar, M.A. & Souri, A. An optimized intrusion detection system for resource-constrained IoMT environments: enhancing security through efficient feature selection and classification. J Supercomput 81, 783 (2025). https://doi.org/10.1007/s11227-025-07253-3

[13] Sharma, N., Shambharkar, P.G. Multi-layered security architecture for IoMT systems: integrating dynamic key management, decentralized storage, and dependable intrusion detection framework. Int. J. Mach. Learn. & Cyber. 16, 6399–6446 (2025). https://doi.org/10.1007/s13042-025-02628-7

[14] Zachos, G.; Mantas, G.; Porfyrakis, K.; Rodriguez, J. Implementing Anomaly-Based Intrusion Detection for Resource-Constrained Devices in IoMT Networks. Sensors 2025, 25, 1216. https://doi.org/10.3390/s25041216

[15] Hafid, A.; Rahouti, M.; Aledhari, M. Optimizing Intrusion Detection in IoMT Networks Through Interpretable and Cost-Aware Machine Learning. Mathematics 2025, 13, 1574. https://doi.org/10.3390/math13101574

[16] Alserhani, F. Intrusion Detection and Real-Time Adaptive Security in Medical IoT Using a Cyber-Physical System Design. Sensors 2025, 25, 4720. https://doi.org/10.3390/s25154720

[17] Khan, M.Z.; Sabur, A.; Ghandorh, H. A Novel Internet of Medical Things Hybrid Model for Cybersecurity Anomaly Detection. Sensors 2025, 25, 6501. https://doi.org/10.3390/s25206501

[18] Naghib, A., Gharehchopogh, F.S. & Zamanifar, A. A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities. Artif Intell Rev 58, 114 (2025). https://doi.org/10.1007/s10462-024-11101-w

[19] Y. Rbah, M. Mahfoudi, M. Fattah, Y. Balboul, S. Mazer and M. Elbekkali, "An Intrusion Detection System For Internet of Medical Things Using Machine Learning Approaches," 2025 5th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Fez, Morocco, 2025, pp. 1-6, doi:10.1109/IRASET64571.2025.11008243.

[20] Jordi Doménech, Olga León, Muhammad Shuaib Siddiqui, Josep Pegueroles,Evaluating and enhancing intrusion detection systems in IoMT: The importance of domain-specific datasets,Internet of Things,Volume 32,2025,101631, ISSN 2542-6605 https://doi.org/10.1016/j.iot.2025.101631.